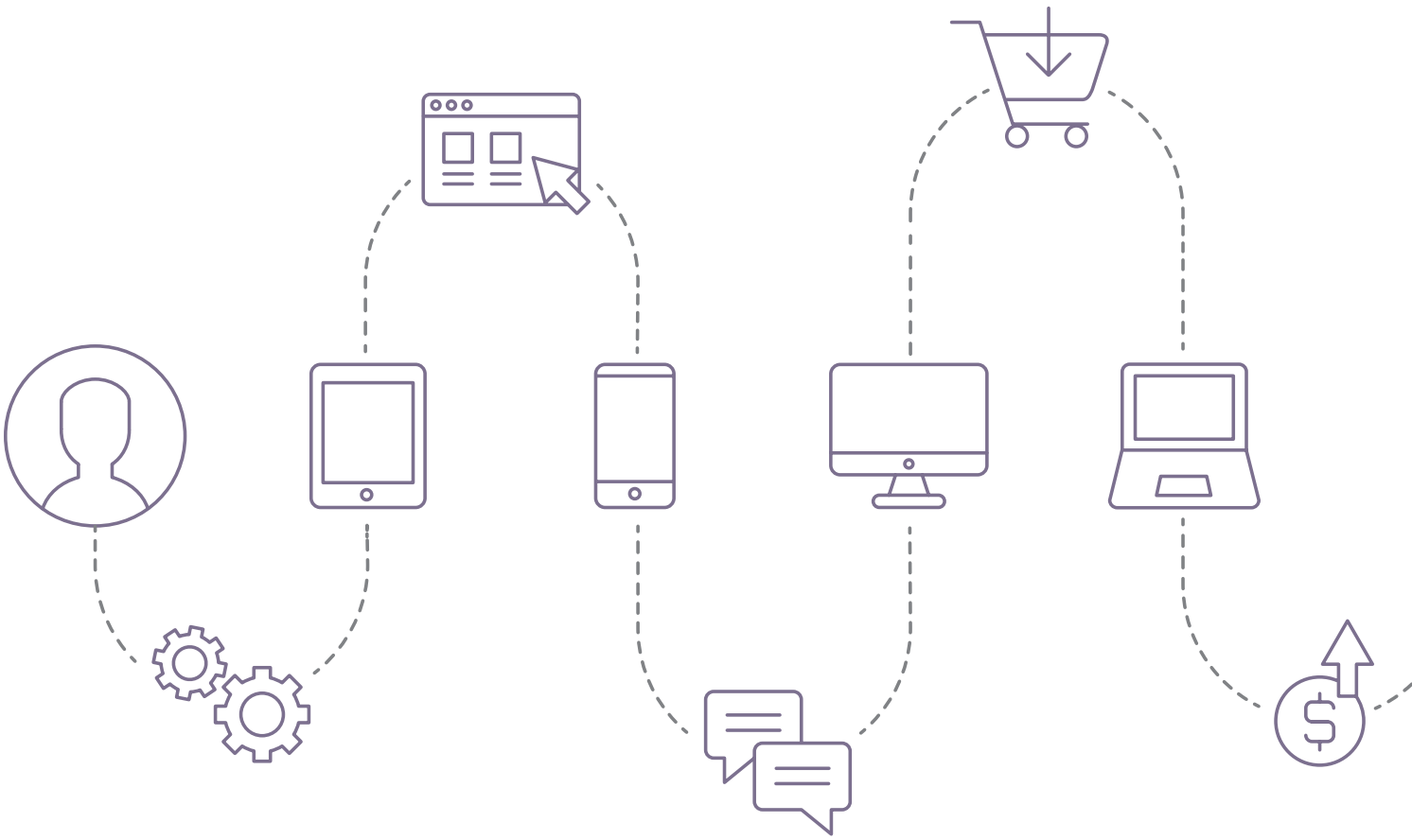
SPEED UP GOOD CUSTOMERS. STOP COMMUNICATIONS FRAUD.

Reduce Fraud Losses.
Exceed Customers' Expectations.

A differentiated customer experience is critical in the hyper-competitive communications market. As part of the customer's overall brand experience, new standards have emerged for frictionless, instant access to sites, services and mobile apps. Yet this experience needs to be weighed against the realities of rising fraud. iovation provides solutions that balance the competing demands of catching fraud, authenticating good customers and providing an outstanding customer experience.



Our Experience

Preventing fraud and protecting communications carriers

Transactions protected by iovation OVER THE PAST 12 MONTHS	**Communications customers**	**All customers**
NUMBER OF TRANSACTIONS PROTECTED	297 million	8.2 billion
NUMBER OF RISKY TRANSACTIONS STOPPED	3 million	514 million
NUMBER OF REPUTATION REPORTS SUBMITTED BY ANALYSTS	336,000	13 million
PERCENT OF DEVICES PREVIOUSLY SEEN BY IOVATION	73%	74%

Types of communications providers that use iovation:

- Wireless
- Wireline
- Cable and satellite
- TV
- Media and pay

Create an Outstanding Experience. Shut Down Account Takeover.

Customer authentication and fraud prevention solutions for communications

The communications industry is fast evolving, and facing a number of challenges. Consumer saturation has been reached in most mature markets, forcing providers to diversify into value-add services to remain competitive such as streaming media, advertising services and digital content. Services cross-pollination have added complexity for carriers trying to manage the same account across multiple offerings. This is problematic because, in this increasingly competitive market, the need to provide a seamless and differentiated customer experience has never been more paramount.

Another key challenge is the need to free up cash in a very capital-intensive market. To this end, many in the industry have begun financing handsets and other assets. This allows carriers to lower the upfront expense of gaining new customers, and it also creates new intricacies within credit risk decisions and introduces new fraud vulnerabilities.

Do you feel like fraudsters find workarounds to every fraud-fighting technique you try? Then you need resources that will evolve with new trends and fraud vectors: smart tools, machine learning and crowd-sourced intelligence. And as always, this needs to balance with what your customers want.

Complicating things further, the massive data breaches over the last decade have provided a flood of stolen credentials and personal data that is now available for pennies on the dark web. Javelin found that compromised Social Security numbers exceeded credit card numbers for the first time in 2017. [4] These trends will undoubtedly accelerate already increasing account takeover (ATO), synthetic and true identity fraud which will, in turn, drive other types of fraud. This not only hits your bottom line but also drives a wedge between you and good customers.

And what do your customers want?

They want secure, easy access to services across all channels at all times. Too much friction at any point and customers could click over to a competitor offering a smoother experience. Your team's job is to make it easier for customers and harder for fraudsters.

Your challenges:

- Stop ATO without adding customer friction
- Fight fraud and abuse across ever-changing vectors
- Improve the login experience without sacrificing security
- Stop hardware losses without losing potential new customers
- Curb rising call center fraud
- Provide a unified login experience across all channels

The solution: Focus on your customer's device

Every transaction. Every engagement with your brand. Every attempt at fraud. They all rely on a web-enabled device. iovation knows the reputation of over five billion devices.

[1] Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent, Javelin Strategy & Research, 2018
[2] Ibid.
[3] Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, Javelin Strategy & Research, 2018
[4] Javelin, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
[5] Digital Lending Fraud, Javelin Strategy & Research, 2017

How iovation Stops Fraud in Communications

iovation's fraud prevention solution uses flexible business rules and advanced machine learning algorithms to stop devices with risky attributes and behavior

Patented technology allows us to spot and stop coordinated fraud rings by determining connected devices and accounts that span businesses and industries without the need of customers' directly identifying personal information. Our comprehensive network of cybercrime fighting professionals submits device reputation reports that detail the type of fraud or abuse a device is confirmed to have committed, such as:

- New account fraud
- ATO
- Call center fraud
- Identity theft
- Prepaid card fraud
- Synthetic identity fraud
- Payment fraud
- Shipping fraud

Your challenges	Our solutions
ATO losses are on the rise ATO causes major losses in terms of lost hardware, chargebacks and lost service revenue. The risk of ATO drops as you increase authentication, but the quality of the user's experience can drop as well.	Strike the balance between security and customer experience with transparent authentication. Users register their devices with ClearKey, which recognizes them in future visits and provides an additional authentication factor, putting a stop to ATO attempts. This extra assurance is invisible and frictionless to customers.
Shipping fraud is increasing Fraudsters often access the order tracking system to see where orders are in the shipping process and will have shipments redirected by the logistics companies.	Our unparalleled ability to track and understand the reputation of a device over time, across different accounts and geographies, allows you to easily spot shipping fraud, and uncover otherwise invisible associations. In tandem, we monitor for risk signals such as high transaction velocities for devices or IP address.
Stop new account fraud, not potential customers Criminals use stolen or synthetic identities to apply for new accounts, making it almost impossible to distinguish fraudulent applications from new customers.	Our patented multi-layered approach to device recognition analyzes thousands of permutations of device attributes to recognize every visiting device while minimizing false positives. Devices with bad reputations – and associated devices – are stopped in real time from opening new accounts.
Commercial account fraud is rising If a fraudster can successfully infiltrate a commercial account, they can create a new sub-account and/or add a location where they can send stolen hardware. Resulting in large losses of equipment that could go unnoticed until the customer disputes the orders.	With device-based authentication customers can register devices to accounts, adding a layer of authentication without adding friction. After the initial pairing, ClearKey recognizes returning devices and transparently authenticates users, allowing a seamless login for trusted customers while shutting down ATO attempts.

How to Provide Fast and Secure Access

The flood of breached credentials over the last decade has made it easier than ever for bad actors to take over good customers' accounts. While communications carriers race to strengthen their authentication solutions, customers expect the best possible online experience, beginning at login.

Your challenges	Our solutions
Call center fraud is rising Fraudsters gather data about customers and then combine high-pressure tactics with spoofing technology to socially engineer your agents to take over customers' accounts or perpetrate SIM swapping.	Multifactor authentication methods in LaunchKey strengthen security both online and offline, without slowing down service. It empowers call center agents to quickly validate callers' devices before providing service.
Credentials are everywhere Nearly 9 billion credentials, account details and passwords have been dumped on the dark web in the last 10 years. Password - and knowledge-based authentication (KBA) systems have been rendered obsolete.	You can no longer rely on single - or even two-factor solutions. With LaunchKey you can layer in multiple authentication options, from transparent and frictionless to interactive and fully integrated.
Current tools miss risk signals Does your customer just want to view their statement? What if they want to make a payment or change their account settings? And if they want to make a large purchase? Each action represents a different level of risk, but most authentication solutions treat them all the same.	Combine LaunchKey's interactive, mobile multifactor authentication with ClearKey's transparent, easy-to-use device recognition for dynamic authentication. The result: The right method at the right time, with the right balance of friction and user experience. The built-in intelligence of this solution acts as a decision engine that drives step-up activity as needed.
Unifying the login experience across all channels The addition of value-added services through industry mergers, acquisitions, and services cross-pollination has added complexity for carriers trying to manage the same account across multiple offerings.	LaunchKey manages all digital and physical authentication processes right in your mobile app. From today's web or mobile app to tomorrow's omnichannel experiences across call centers, account login or even IoT devices. LaunchKey provides the broadest set of user-selectable multifactor authentication methods and unifies the customer experience.

Rethink Authentication and Improve Access

Armed with billions of user credentials breached over the past decade, and plenty of patience, fraudsters will compromise not just single accounts, but whole databases. Legacy authentication systems reliant on passwords, or text-based, one-time passwords alone don't stand a chance. It's time to move on.

Overcoming modern fraud and authentication problems – while improving customers' service experiences – calls for a completely new way of thinking. LaunchKey anticipates this challenge with:

- **Omnichannel flexibility:** Today, authentication varies by the channel. On the web, customers enter their username and password, and possibly a one-time password. They enter the same credentials on your mobile app, but with a tiny, typo-prone keyboard. When calling for help, they answer KBA questions. Imagine a time when every channel will use the same simple authentication method: The user's device.
- **Decentralized architecture:** Remove the target and hackers have no way of stealing and reusing identity information on a large scale. Older authentication systems use large centralized credential stores that are a very lucrative target. We separate the authentication process from the application, reducing your liability and keeping encrypted credentials – and risk – dispersed on each end user's device.
- **Updatable platform:** New authentication methods will enter the mainstream soon. Users will be able to authenticate with their voice, heartbeat, iris, or more. We designed LaunchKey as a mobile multifactor authentication platform that will readily adapt to new methods with modification to its SDK.

To remain competitive, you must balance experience with security. That's what our products are built to do. Learn more about the solutions mentioned in this industry brief by visiting **iovation.com**.

ClearKey

Provide your customers with a transparent authentication method that stops ATO but doesn't slow them down.

LaunchKey

Increase security, kill passwords and provide your customers with mobile multifactor authentication.

FraudForce

Establish fraud risk based on suspicious behavior and risky data. Uncover more fraud through device associations.

SureScore

Predict the outcome of any given online transaction, even if you have no history with the customer involved.

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation.com

Global Headquarters

iovation, a TransUnion company
555 SW Oak Street, Suite #300
Portland, OR 97204 USA

PH +1 (503) 224 - 6010
FX +1 (503) 224 - 1581
EMAIL info@iovation.com

United Kingdom

PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation®
A TransUnion® Company